8010 AT&T Technical Journal
73(1994)Sept./Oct., No.5, New York, US

Secure Network Access Using Multiple Applications of AT&T's Smart Card

Stephen A. Sherman
Richard Skibo
Richard S. Murray

Fraud amounting annually to billions of dollars occurs due to the failure of conventional network access security systems, including data, voice, and credit card authorization networks. At the same time, consumers demand greater convenience in their daily lives, where a multitude of passwords and personal identification numbers, badges, keys, and other devices have become unmanageable. In response to the obviously conflicting needs, AT&T has developed a credit card sized device, the contactless AT&T Smart Card. By means of an internal microprocessor, the card provides the secure partitioning of authentication codes and data files, as well as encryption capabilities, using the data encryption standard. This paper provides a basic description of the card technology, and the overall architecture of securing access to multiple networks with the AT&T Smart Card.

Introduction

The design of network security systems requires a balance between how secure the system can be and how easy it is for a legitimate network user to access it. This balance is increasingly difficult to maintain as costs from fraud and theft escalate, while users demand even simpler and more convenient access. The AT&T Smart Card uses an embedded processor that gives both the system designer and the system user a powerful authentication tool, yet it looks and feels like an ordinary credit card.

This card provides secure access to multiple applications using a combination of security systems for access. A single card could provide:

- Physical access, such as opening doors to a building or vehicle, or turning on a computer or other restricted equipment;
- Financial access, such as withdrawing cash from a bank;
- Credit access, such as validating its use as a credit card;
- Health care information access, such as providing information on health care records and insurance eligibility; and
- General data access, such as getting permission from a security server to access a variety of databases.

With the AT&T Smart Card, the user no longer has to maintain a personal library of personal identification numbers (PINs) and passwords. At the same time, security system designers and administrators are assured that their individual network authentication schemes are kept private and secure. Security system design now can focus on a user having only a single card (also called a "token") or two for a variety of purposes. Such a card could be:

- A student identification (ID) card that provides indentification, as well as access to a student's dormitory, library, dining hall, and gymnasium;
- An employee ID card that provides not only access to company buildings, but also company equipment, such as computers, copying machines, the company library, and other services and facilities;
- A multi-function smart credit card that provides not only identification, but also secure credit or debit transactions, such as the student ID mentioned above that can also be used as a charge card at the school bookstore, library copying machines, and snack bars; and
- Stored-value cards, for example, cards that can be pre-paid for specific functions, such as telephone calls—a particularly popular

Panel 1. Acronyms Used in This Paper

ASIC—Application-specific integrated circuit
ATR—Answer to reset, the information returned by a Smart Card when power is applied.
CBC—Cipher block chaining. One of various modes of DES encryption.
DES—Data encryption standard
DF—Dedicated files
ECB—Electronic code book. One of various modes of DES encryption.
EF—Elementary files
EEPROM—Erasable electronic programmable read-only memory
IC—Integrated circuit
ID—Identification
ISO—International Organization for Standardization
MAC—Message authentication code
MF—Master file
OFM—Output feedback mode. One of various modes of DES encryption.
PIN—Personal identification number
PTS—Protocol type select
RAM—Random access memory
ROM—Read-only memory
SAM—Security application module
SF—Sub-dedicated files
T-0, T-1—Asynchronous, half-duplex transmission protocol defined in ISO Standard 7816-3

use in Europe, or highway tolls. Such a card has the capacity to store "electronic money" that can be debited as the card user spends it.

Growth of Smart Cards

Smart cards are a subset of the rapidly growing integrated circuit (IC) card industry. More than 200 million IC cards have been deployed, mainly for providing a convenient method of storing monetary value. About 10 percent of these IC cards are "smart" cards, that is, their processing capabilities extend beyond just debit/credit functions. But the number of smart cards is increasing, stimulated by four conditions:

- A continuing decline in the cost of microprocessors;
- An increase in fraud as conventional security techniques—based on passwords, PINs, and magnetic stripe credit cards—fail;
- A dramatic trend away from centralized security schemes and toward distributed security access systems, in which a portable security token, such as the AT&T Smart Card, is invaluable; and
- The confusion and resistance of network users and consumers who are overwhelmed by a proliferation of various cards, passwords, PINs, and physical keys for individual systems.

By combining the functionality of the various authentication tokens, the AT&T Smart Card greatly simplifies the daily life of the network user—while providing enhanced security.

Overview of Smart Card Technology

Essentially an 8-bit computer inside a credit card, the contactless AT&T Smart Card contains a proprietary operating system and either 3 kilobytes or 8 kilobytes of user-accessible, non-volatile memory. The card merges innovative concepts in electrical and physical design, as well as in materials engineering. A functional diagram of the AT&T Smart Card is shown in Figure 1. The main components of the card are:

- An 8-bit microprocessor with on-board read-only memory (ROM), erasable electronic programmable read-only memory (EEPROM), a small amount of random access memory (RAM) available from the operating system, and enhanced security functions;
- Power-conditioning circuitry;
- Custom application-specific integrated circuit (ASIC), for data translation and power conditioning; and
- Patented contactless reader/writer capacitive plates and inductive power transfer coil.

Why It's Smart. The AT&T Smart Card's EEPROM supports a minimum of 100,000 read/write cycles. In addition to containing a complete computer system, the card meets all relevant international and domestic standards for magnetic stripe credit cards, including thickness, life-cycle bending, and the ability to be handled by automated credit card machinery.

The AT&T Smart Card can communicate at up to 19,200 bits per second with a reader/writer machine, the device that reads data from, or writes data into, the card. The card supports the International Organization for

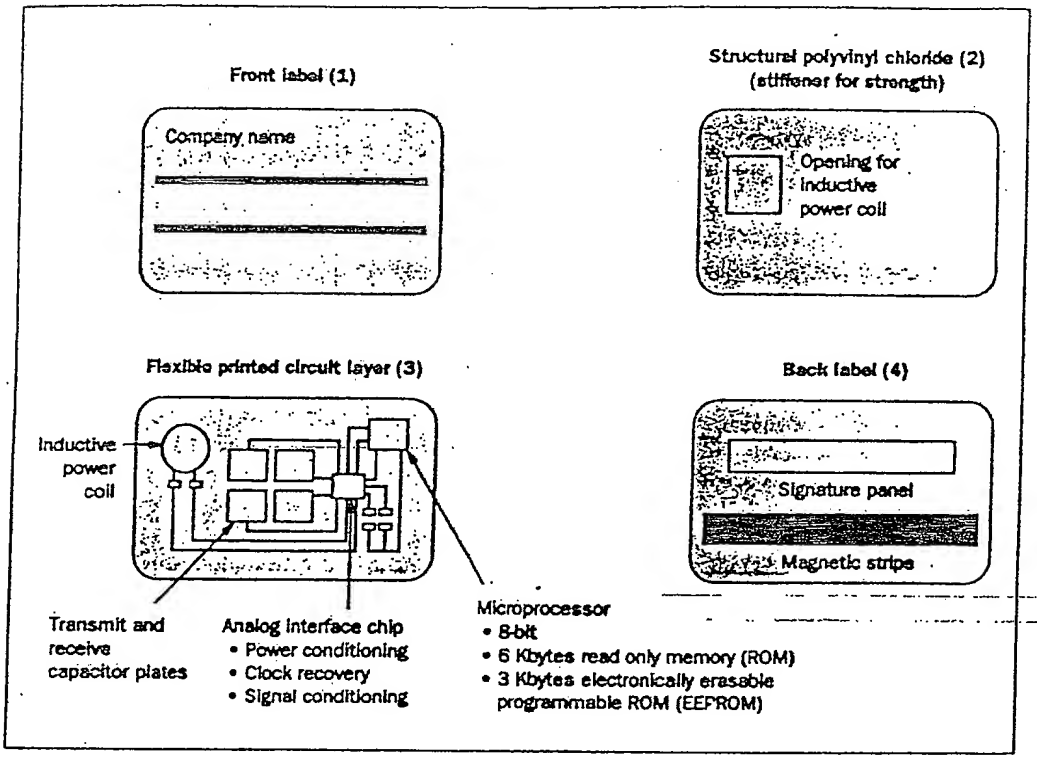

Figure 1. The AT&T Smart Card includes a 8-bit microprocessor with on-board read-only memory (ROM), erasable electronic programmable read-only memory (EEPROM), random access memory (RAM) available from the operating system, and enhanced security functions. It also has power-conditioning circuitry, custom application-specific integrated circuit (ASIC) for data translation and power conditioning, and patented contactless reader/writer capacitive plates and inductive power transfer coil.

Standardization (ISO) specification for answer to reset (ATR) (the information returned by a Smart Card when power is applied), and protocol type select (PTS), for T=0 and T=1 protocols (used to transmit data to and from the Smart Card in character or block mode, respectively). The card's operating system resides within the single-chip microprocessor. All access to it's memory must be through the card's microprocessor, which arbitrates the request based on the permissions that were installed during the creation of the card's protected file or directory.

In describing the features of the contactless AT&T Smart Card, it is important to distinguish it from the contact-type IC cards in use today, most of which:

- Primarily support a single application,
- Require physical contact with a reading machine, and
- Contain only an EEPROM memory device, with limited or no security functions.

In contrast, the AT&T Smart Card:

- Supports multiple applications of either single or multiple vendors,
- Doesn't require physical contacts in order to be read by a machine, and
- Has a processor-supported operating system with a variety of security techniques and levels of security.

Why It's Contactless. In addition to the microprocessor, the most obvious difference between the AT&T contactless smart card and a contact IC card is in the physical and electrical interface.

Typical Contact Card. The contact-type interface uses an eight-position contact located at one corner of the card. The exposed, external interface provides an easy point of access for damage from static discharge, and this external interface can be physically damaged by abrasion, corrosion from perspiration, and various environmental chemicals. An inexpensive contact card reader also uses delicate contacts, which may be damaged by extensive use, abuse, vandalism, or other misuse—all of which can result in the user being denied service. To make the contact-type reader robust, a motorized transport is required, at the insertion slot of the reader machine, to take the card away from the user for reading. While desirable in certain applications, such as automatic teller

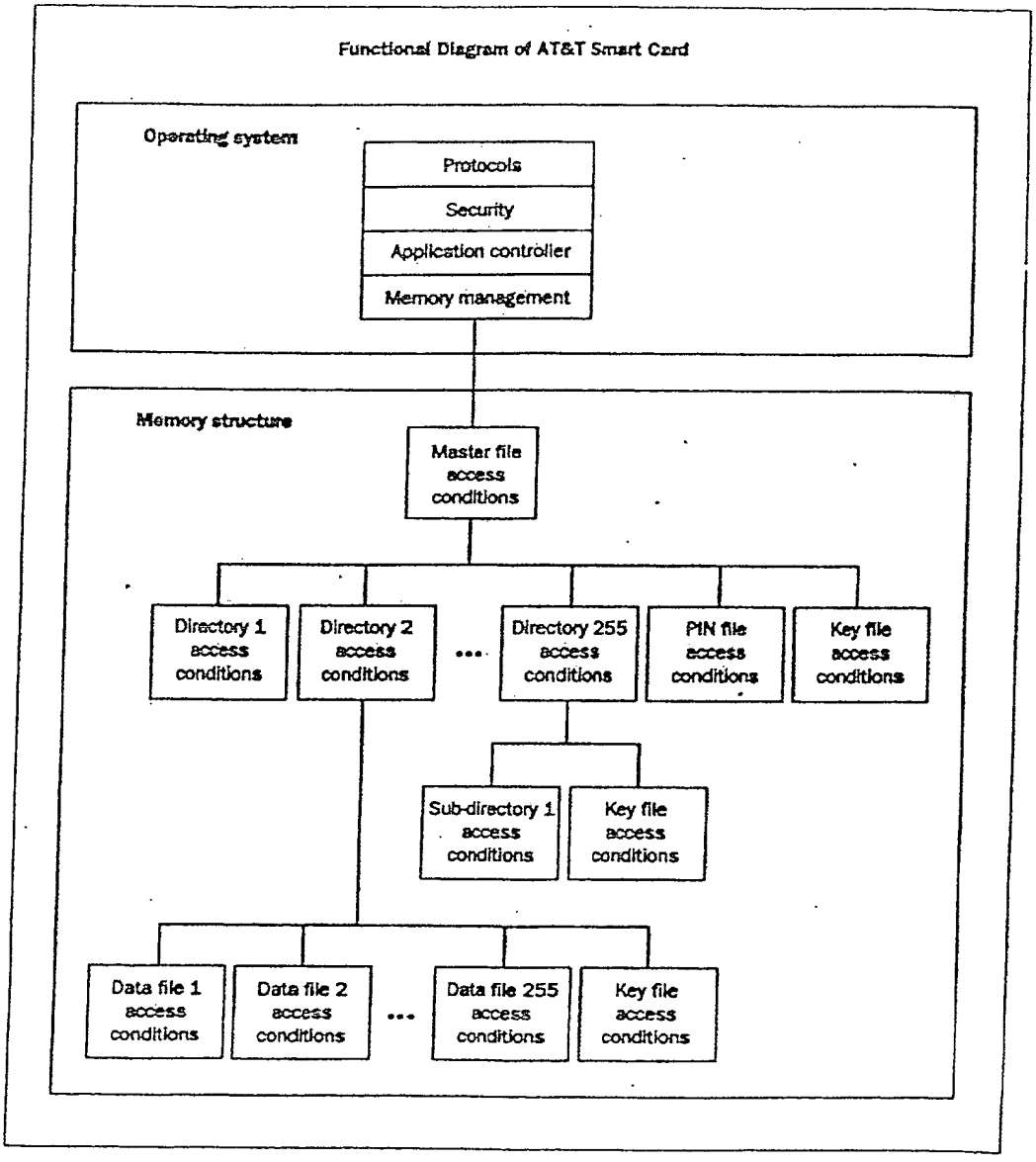

Figure 2. The AT&T Smart Card has an operating system that implements a hierarchical file system. The physical separation of files is possible using different branches of the hierarchy. Access permissions, such as read, write, and execute, can be assigned on a per-file or per-directory basis. The hierarchical structure permits a card provider to offer various levels of access and functionality, as well as permitting multiple applications providers to offer a variety of services—all on a single card.

machines and vending machines, this mechanical complexity can add significant cost and bulk to a reader machine. This motorized transport also is annoying to card users when the machine erroneously "eats" the card, due to either incorrect data or a mechanical glitch.

AT&T's Contactless Interface. In contrast, AT&T's contactless interface uses an inductive coil for power transfer and capacitive plates for information transfer. These components transfer data to a matching set of components in the reader/writer machine interface. Inductive power transfer and capacitive data transfer provide a highly reliable and inexpensive circuitry.

All card-related components are laminated beneath the surface of the card; the corresponding

reader components may be encapsulated beneath a plastic housing, as required. No external contacts are visible to the user or to a potential vandal or hacker.

The components required by a reader machine to interface with the contactless AT&T Smart Card include a coil, a custom ASIC, several passive components, and approximately four square inches of circuit board space to accommodate the capacitive transfer plates and the associated circuitry. When produced in quantity, the cost of these additional components is quite minimal. The actual cost to the end user depends on a variety of parameters, including the method by which the reader manufacturer incorporates the contactless interface and the overall system parameters. In general, the incorporation of the contactless interface into an existing magnetic stripe reader design is significantly less expensive than a conversion for a contact interface.

Operating System Security

The AT&T Smart Card was designed with the fundamental requirement that information be securely accessed and stored on the card. This is possible through the card operating system, which implements a hierarchical file system as shown in Figure 2. The physical separation of files is possible using different branches of the hierarchy. Access permissions, such as read, write, and execute, can be assigned on a per-file or per-directory basis. The hierarchical structure permits a card provider, such as a corporation issuing employee ID cards, to provide various levels of access and functionality. In addition, the structure permits multiple application providers (vendors) to offer a variety of services—all on a single card.

For historical reasons, directories within the smart card are called either dedicated files (DF) or sub-dedicated files (SF). Data files are called elementary files (EF). The root directory is called the master file (MF).

Secure Multiple Applications. Each provider or application that an AT&T Smart Card supports must be guaranteed to have its own high degree of security. Therefore, the card features multiple directories, and every application is contained in its own dedicated file and has its own set of security attributes, thus completely isolating it from all other applications. An application may use one dedicated file, with multiple sub-dedicated files and elementary files, to protect data from other applications. All information is fully partitioned and secured, therefore, through the hierarchical file system. This allows the card to support added services and expanded functionality, even after it has been issued, while still maintaining complete data integrity and security for all applications, whether provided by one or more vendors.

Restricted Databases. As the smart card is essentially a highly secure, but portable and robust file system, there is no intrinsic concept of user ownership. Rather, through the use of PINs and keys (binary numbers used to encrypt and decrypt information), it is possible for each user to access different subsets of files and directories in the card's database. A file present on all cards issued by a provider, for example, can become readable only through the valid presentation of a PIN or key known to one group of users, but not available to another group. This allows information to be available on all cards, yet hidden to various users, based upon the card provider's judicious disclosure of the appropriate PINs or keys.

The AT&T Smart Card is generally configured to allow access to all applications by use of a single PIN known by the cardholder, plus various keys known by each application owner. To segment applications, unique directories normally are assigned to each application, with each application assigned unique security keys.

Such a card could be the employee ID issued to workers in, for example, a munitions plant. An employee ID card could grant general access to the plant grounds, but restrict access not only to a certain building, but to specific areas within that building. In addition, the card might restrict access not only to certain computers or other facilities within that building, but even to certain files and directories within the computer's database. The card also could contain the employee's medical information, job history, signature, encoded photo, and other pertinent data. It even could be used to withdraw supplies from the company stockroom and to charge meals at the company cafeteria.

Once the security required for an application is determined, the access conditions of the card associated with any created files or directories can *never* be changed for that card. While certainly requiring more up-front analysis and design for an application, this mechanism ensures that no security limitations can ever be introduced by some later modification of the card. Additionally, even though the properties of the data encryption standard (DES) used by the card make exhaustive key searches by a hacker or vandal quite unlikely, and

certainly very expensive, if an access key is discovered by an unauthorized user, the access key could be changed in the reader machine. Such a change would be accomplished by the use of another access key. Four such keys can be created in each application directory. Of course, these additional access keys would have to be reserved only for this function and not be used in other operations, where they could be inadvertently disclosed.

Levels of Security. The AT&T Smart Card provides built-in functionality to perform varying levels of security. The following describes the basic security functionality contained on the card:

- Files protected by a *personal identification number* are only accessible after the user presents a valid PIN. The card compares the user-entered PIN with a previously shared value. To protect against "PIN guessing," an internal counter tracks the number of successive, unsuccessful attempts. Once the configurable threshold is reached, no further PIN attempts are accepted by the card, and the card is essentially disabled. The card can be configured so that it could be either permanently disabled or temporarily disabled until some administrative security procedure is performed on it.
- Data transferred to and from files also can be protected against tampering by appending a *message authentication code* (MAC). This code prevents the undetected modification of any data transferred to or from the card. The MAC is calculated using the DES cipher block chaining (CBC) mode on the data.
- Authentication requires the presentation of a valid DES *encrypted value*. To protect against "key guessing," an internal counter tracks the number of successive, unsuccessful attempts. Once a fixed threshold is reached, no more authentication attempts are possible, and the card can be either permanently or temporarily disabled. The value is calculated using the DES electronic code book mode. The key is never directly disclosed in un-encrypted form, in order to prevent theft. Rather, a value determined either by the card or by the network is encrypted with the key and passed back to the other for validation.
- Finally, all communications with the card can be performed in *encrypted mode*. This mode eliminates any unauthorized access to information when reading from or writing to the card. Further, a MAC, calculated using CBC mode, also is appended to the encrypted message. All information is encrypted using the DES output feedback mode.

Table I summarizes the access conditions, from least restrictive to most restrictive, which can be assigned to the access of every file or directory on the AT&T Smart Card. Additionally, several of the access conditions can be combined.

Validation Mechanisms

The AT&T Smart Card provides for two types of validation:

- *External validation*, in which the users authenticate themselves to the card, and the card then validates the user, and
- *Internal validation*, in which the card authenticates itself to the network, and the network then validates the card.

In this paper, we regard *authentication* to be the process of a user claiming to be authentic, i.e., being whomever he or she claims to be. Signing a check would be such a process. *Validation* is then similar to the teller validating the signature and, thus, the signer's claim of authentication. Another example is an employee claiming he or she is an authentic employee by showing a company pass to a security guard, who validates the pass after inspecting it. In the field of encryption, however, the two terms often are used interchangeably.

External Validation. With external validation, users must prove their knowledge of the keys contained on the Smart Card without, of course, disclosing the key to unauthorized users. As such, keys can never be communicated un-encrypted. Once the external validation operation is successfully completed by the user, access to those operations requiring external validation is possible. The basic process of external validation is as follows:

1. When the card is inserted in the reader machine, the machine's processor asks the card to generate a random number. The reader machine then informs the user what the number is.
2. Via appropriate buttons or keyboard commands on the reader machine, the user DES encrypts the random number, using electronic code book (ECB) mode, with what should be the appropriate key. The user then stores the encrypted random number in the reader machine.
3. The user then instructs the reader machine to send the encrypted random number to the card.

Table I. Access permissions available on the AT&T Smart Card

Access code	Access conditions. Applied to read, update, create, delete, and other operations
ALW	Always possible
PUI1	Valid presentation of PIN, once per session
PUI2	Valid presentation of PIN, once per access
PRO	A message authentication code (MAC) is appended to all data communications and validated
AUT	External authentication
ENC	All data communications are encrypted, with a MAC also appended to message
PUI1/PRO	Combination of previous items
PUI2/PRO	Combination of previous items
PUI1/AUT	Combination of previous items
PUI2/AUT	Combination of previous items
PUI1/ENC	Combination of previous items
PUI2/ENC	Combination of previous items
NEV	Never possible except through operating system primitives

4. The card performs DES encryption on the random number, also using ECB mode, with the appropriate key stored in its memory, and compares its results with the encrypted random number passed to the card by the user.
5. Based upon the comparison, the external validation operation will succeed if the user and card used the same key. Otherwise, the operation will fail.

It is important to note that an un-encrypted key is *never* transmitted between the card and user. Further, since the random number is generated by the card, it is not possible to use a previously successful random number to authenticate access. This eliminates the potential of a "replay attack." In order to deter the persistent attacker waiting for the same random number, the card will not generate a new random number if an external validation command has not been issued in the interim. In any event, the random number is 64 bits long, so the attacker would wait quite some time before the same random number was again presented.

Internal Validation. The basic process used for secure network access follows a similar procedure for internal validation. In this case, however, the network must determine if the user possesses the appropriate key, which is stored in the user's card. The basic process of internal validation is as follows:

1. When the card is inserted in a reader machine to access a network, the network generates a random number and sends it to the card, via the reader machine.
2. The card DES encrypts the random number, using ECB mode, with the appropriate key.
3. The card sends the encrypted random number to the network, via the reader machine.
4. The network performs DES encryption, also using ECB mode, with the same random number and, presumably, the same key, and compares the card's encrypted random number with its encrypted random number.
5. Based upon the comparison of the two encrypted random numbers, the network allows or disallows access.

It should be noted that although these procedures seem to place a great deal of burden on the reader machine, the machine itself does not have to be a complicated device. It could be attached to a serial port of a processor, which could perform all the above internal and external validation tests in software.

Again, note that the un-encrypted key is never transmitted between the network and user. In actual operation, all access to the card would also be PIN protected to prevent the use of a lost card.

Off-Line Security. Validation also supports a distributed "off-line" security environment. For example,

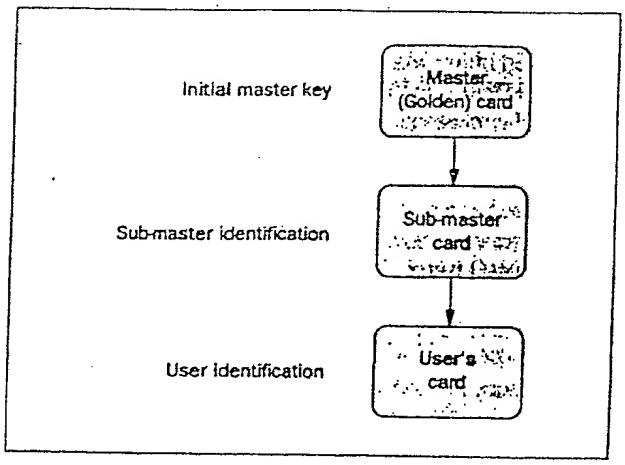

Figure 3. Through the use of innovative key management techniques, a key hierarchy can be created for the AT&T Smart Card. A master key can be created, and by using a word or words, whether it be a user identification, phrase, name, etc., as a "seed," a set of lower-level keys can be created, resulting in a unique user key.

typical building security systems protected by card access require a large network of cables connecting door readers, door controllers, and host computers. When a card is presented to a door reader, the ID number is transmitted via the network to a host computer. After the ID number is verified, the host computer sends a signal to the door controller to open the door.

By allowing the card to perform the comparison against a stored or internally calculated number, the card can essentially decide if it is allowed permission. In this simple example, a door reader would issue a door ID number to the card, the card would search an internal database of accessible door IDs, and then decide locally, that is, by itself, whether to open the door. This removes the need for a significant network infrastructure within the building. PIN verification, or some other more sophisticated method, also could be implemented to protect against lost or stolen cards. Encrypted versions of this example can be created for even higher security.

Concerns of Databaseless Key Management

As stated earlier, the AT&T Smart Card is a natural adjunct to a system of off-line authentication. By storing the key within the Smart Card, the user does not need to know the key, or keys, so no user can in any way compromise the security of the system.

In the simplest realization of this system, a common key is stored both in the user's AT&T Smart Card and in a host security application module (SAM), which can also be a host smart card. Using the common key, the user's Smart Card and the host SAM can perform the processes of internal and external authentication described earlier.

Unfortunately, this process has serious drawbacks. If the common key is compromised in any fashion, the entire distribution system must be revamped, since every user's AT&T Smart Card, as well as every host SAM within the system, uses the common key. In addition, this process would preclude the revocation of security rights to a particular user, since his or her key would be identical to every other user's key.

An improvement to this method is to assign each user a separate and unique key. The security application would require a database of every key, mapped to some unique user ID number. In this manner, the SAM would be able to perform an authentication on a specific user, using the user ID as an index into the table of keys. Once the key is retrieved, the same bilateral authentication process is performed to validate the user.

While this system is a significant improvement over the common key system, the storage of all the keys in the authentication device creates some extreme difficulties. For example, assuming 300,000 employee ID holders of a large corporation, each of them requiring an 8-byte key, each SAM would require a minimum of 2.4 Mbytes of storage. The expense and complexity of the SAM, therefore, becomes very significant.

In a distributed enterprise, the administration of such a key system would be extremely difficult, especially when one considers the thousands of SAM devices that would be required to accept a particular Smart Card.

AT&T Databaseless Security System. The patented AT&T Databaseless Security System removes these limitations. This particular system, through the use of innovative key management techniques, permits the creation of a key hierarchy to allow not only the simple and effective distribution of keys, but the creation of a management hierarchy. This hierarchy is shown in Figure 3.

In this innovation, a master key card is created in a secure environment. Using any word or words, whether it be a user ID, phrase, name, etc., as a "seed," a

Table II. Space requirements for various biometric data storage.

Biometric method	Feature extraction mechanism	Ultimate data size for realistic authentication
Photo image	Data compression	1000-1500 bytes
Signature	Stroke analysis	500-1000 bytes
Voice template	Digital signal processing	1000-2000 bytes
Fingerprint	Synactic and other processes	500-1000 bytes

set of lower-level keys can be created, ultimately resulting in a unique user card. By associating a secret DES key physically with a card, it is possible to distribute keys throughout the security system as physical cards. This could mean that a user or system administrator actually has no knowledge of what the key is, but only has possession of the appropriate level key card. Keys can then be tracked as physical entities that can not be duplicated, simplifying greatly the security auditing and controls process.

For example, to validate a user, a security application module would only need to know the "seed," perhaps some user ID. From this, the administrator's card would internally synthesize the user key, and then execute the authentication process as required. The synthesis process, performed by the AT&T Smart Card, basically is the conversion of very long keys, generally 10 times longer than the user key, to a unique user key via mathematical operations.

With the concept of a databaseless key management system, the development of a key management hierarchy using the AT&T Smart Card becomes a deterministic process. This, coupled with the features within the card's operating system, allows remote administration of multiple applications on the card over the entire useful life of the card.

Biometric Authentication

A common method of providing additional security when using a Smart Card is the implementation of a PIN. This number is stored in a secure fashion on the Smart Card. Although this mechanism is a potent security feature, it still can be circumvented by clever espionage. The most obvious breach of security involves users who write their PINs in less than secure locations, offering easy opportunities for compromise.

A higher level of security can be achieved using *biometric authentication*. In this process, some basic physical characteristic of the user is required to validate the user's authenticity. A simple example of biometric authentication is a person's signature. Upon request, a user would be required to sign a document, such as a check. The biometric data, in this case the signature, is then viewed by a validation mechanism, a bank teller, and used to validate the user's authenticity to allow an application to be performed, such as dispensing money.

More sophisticated methods of biometric authentication in use today include retinal scans, fingerprints, hand geometry, voice prints, facial scans, signature comparison, etc. The AT&T Smart Card provides a convenient and portable method for a person to carry and present a biometric standard securely stored in the card. The storage capacity of the card limits the size of the biometric template. By means of various algorithms, data compression methods, and biometric capture and analysis schemes, however, biometric authentication using the card becomes economically viable. Table II shows various biometric methods and the projected data size for card storage.

In particular, the AT&T Smart Card organization has demonstrated the capabilities of using the card to provide image compression, digital color-photo imaging for physical security, voice template for local automatic teller machine access, fingerprint data storage, and signature profile data storage.

Multiple Application Smart Card

Figure 4 describes a typical Smart Card file layout for the implementation of multiple applications. The card holder would typically be allowed access to any application after entering a valid PIN. As such, the PIN file is placed in the master file, or root directory, so that a single PIN unlocks card access (based upon security requirements, PIN entry may be by-passed). Also placed in the master file are access keys. These keys are known

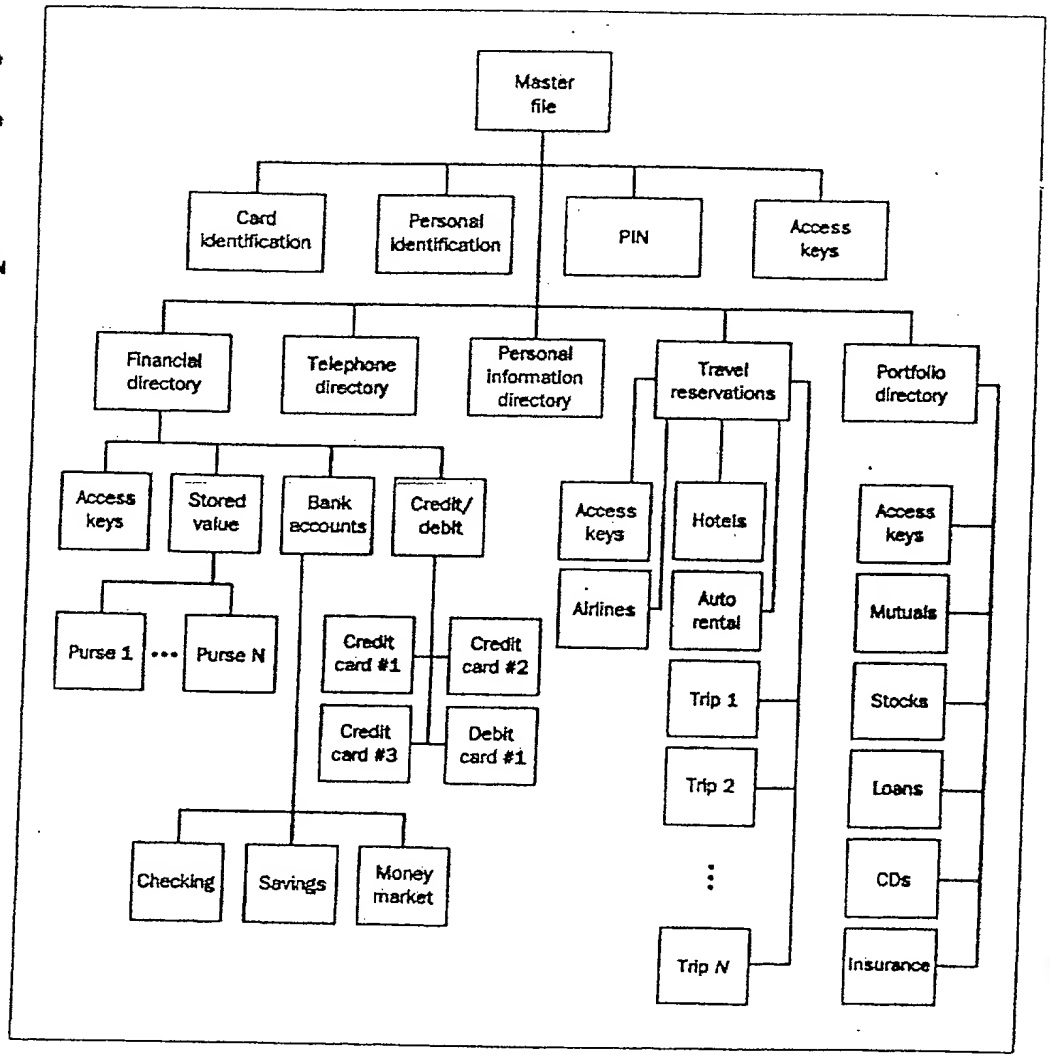

Figure 4. A typical AT&T Smart Card file layout for the implementation of multiple applications would allow the card user access to any application after the valid entry of a PIN. The PIN file is placed in the master file, or root directory, so that a single PIN unlocks card access. Access keys also are placed in the master file. These keys are known only to the card provider, who manages the addition or deletion of new applications.

only to the card provider, who manages the addition or deletion of new applications.

Once a new directory has been created, unique access keys are assigned by the application owner. This allows the application owner to secure any information from the card provider, who knows the access keys in the master file, or from other application owners, who own unique access keys in other directories. For example, the owner of a financial application directory would not want the owner of a travel reservations application to be able to modify the stored dollar balance in the card's electronic "purse." Otherwise, it would be possible to fraudulently modify the dollar amount in the purse, in effect, mint money. It may be desirable, of course, for hotels in the travel reservations application to *read* a customer's credit card account in the financial application directory, or to *debit* that account, while still preventing any increase in the electronic funds available.

Multiple applications on a single card also offer the ability to share both the cost of physically issuing and administrating the card, and the cost of the card itself. This also promotes the concept of providing new

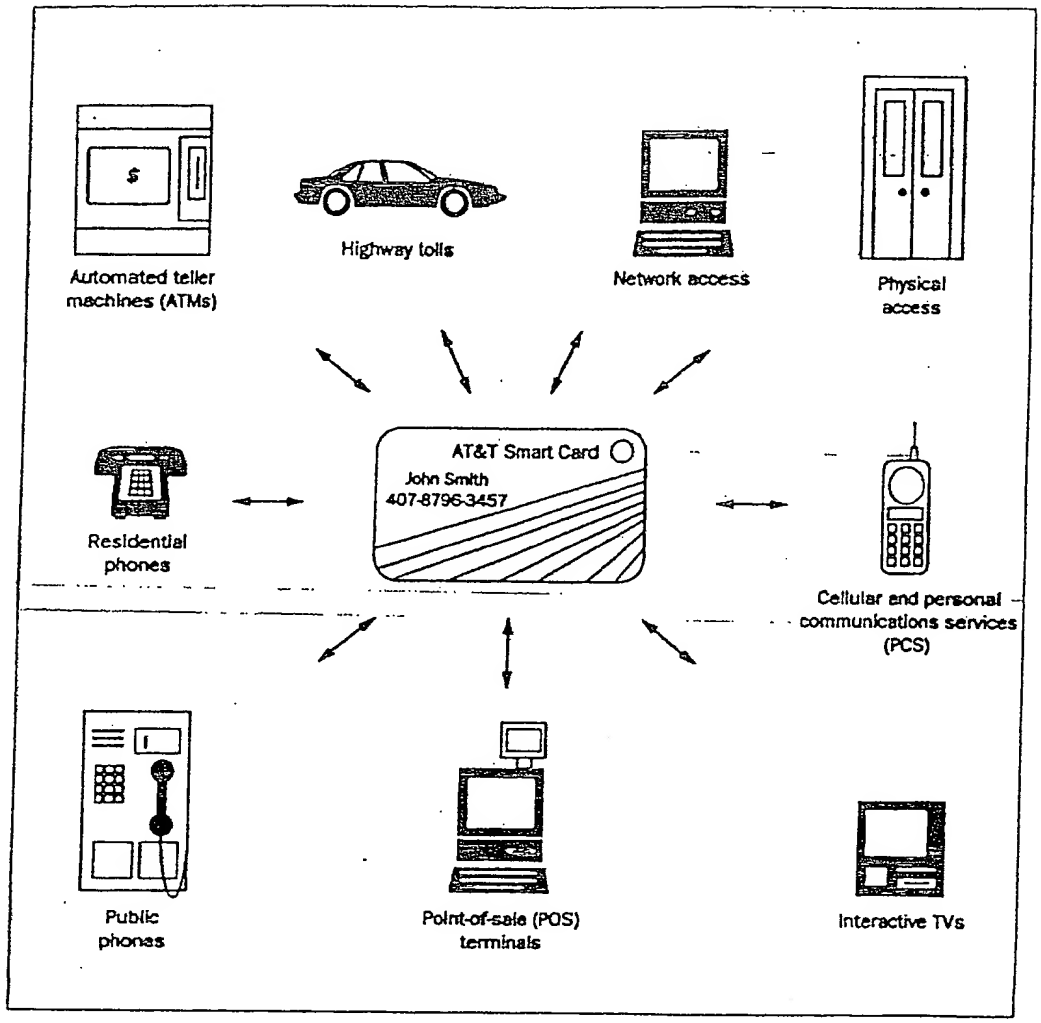

Figure 5. Once a card is issued as a security device, multiple applications can be added, enabling an extremely easy-to-use authentication card device. A future consumer or network user may eventually carry one or two multiple application AT&T Smart Cards to manage secure access to various networks, replacing the nine to 12 cards the average person carries.

features and services at a later date, without the expense of physically issuing a new card.

Conclusion

Once a card is issued as a security device, multiple applications can be added, enabling an extremely easy-to-use authentication card device. A future consumer or network user may eventually carry one or two multiple application smart cards to manage secure access to various networks, replacing the nine to 12 cards the average person carries today.

One card may appear as a multi-function employee ID card (see Figure 5), or as a campus ID card, containing all the necessary security access permissions and other critical data. The other card may be a personal financial card, containing a combination of personal credit, debit, and telephone calling cards, encoded photo and signature, as well as access to personal vehicles and even the user's home or apartment.

The contactless AT&T Smart Card provides a crucial building block in network design and administration, as security systems continue to evolve in a distributed network environment, and consumers demand quicker and easier access to these systems.

Acknowledgments

The authors would like to acknowledge the following people for useful technical discussions that helped develop this manuscript: C. Grullon, D. Claus, R. Flynn, K. Murphy, R. Saksa, J. Snavley, G. Stanley, W. Thompson, R. Till, R. Whitman, L. Atkinson, A. Zahavi, A. Kachhy, R. Carlisle, J. York, R. Mandelbaum, and K. Borg.

References

1. Federal Information Processing Standards (FIPS) Publication 46 "Data Encryption Standard."
2. Federal Information Processing Standards (FIPS) Publication 81 "DES Modes of Operation."
3. AT&T Smart Cards Function Library 4.1.
4. AT&T Smart Cards Programmer's Manual 1.1.
5. International Organization for Standardization (ISO) Document Standard 7816-3
6. American National Standards Institute (ANSI) Standard X3.92-1981, Data Encryption Algorithm

(Manuscript approved June 1994)

Stephen A. Sherman, *former director of product realization for AT&T Smart Card Systems and Solutions, is manufacturing and engineering manager for the AT&T Network Wireless Systems Product Realization Center. Mr. Sherman joined AT&T in 1984. He has a B.S. degree in mechanical engineering from Georgia Institute of Technology in Atlanta and is the past chairman of the U.S. Smart Card Industry Association.*

Richard Sklbo *is a systems engineering manager at AT&T Smart Cards Systems and Solutions. He has a B.S.E.E. degree and an M.S.E.E. degree from Lehigh University in Bethlehem, Pennsylvania. He joined AT&T in 1986.*

Richard S. Murray *is a systems engineer at AT&T Smart Card Systems and Solutions. He has a B.S. degree in industrial engineering from Rutgers University in New Brunswick, New Jersey; an M.B.A. degree from Purdue University in West Lafayette, Indiana; and an M.S. degree in computer science from New Jersey Institute of Technology in Newark, New Jersey. He joined AT&T in 1981.*